critical software

CASE STUDY | ENERGY

Building an Audit-Ready Cybersecurity Baseline

How a large energy-sector client transformed a fragmented requirements landscape into a structured, compliant, and audit-ready cybersecurity baseline.

The challenge

An energy-sector client faced a severe compliance breakdown in its ability to demonstrate cybersecurity compliance with critical standards, regulations, and customer obligations.

Over 500 cybersecurity requirements lacked consistency and traceability. Requirements were mislinked, duplicated, or entirely unmapped — creating issues for both northbound and southbound traceability. Requirements were written with no standardized methodology, leading to ambiguity and loss of control across the project.

The absence of industrial automation principles in requirements management affected the reliability of solutions. The organization was unable to prove compliance with key frameworks, including NERC-CIP , IEC 62443 and other regulatory and contractual obligations

© Critical Software

The solution

A team of requirements engineers worked closely with the customer's cybersecurity engineers to perform a full-scale verification of every system requirement. Each requirement was reviewed, corrected for logical consistency, and restructured in line with industrial automation principles.

Critical Software analyzed northbound and southbound linking for all system requirements. Where gaps were identified, new requirements were suggested to ensure complete and verifiable compliance coverage.

Key elements of the engagement included:

- Full verification and logical restructuring of system requirements in line with industrial automation principles.
- Northbound and southbound traceability analysis, with gap identification and targeted remediation.
- Analysis of customer product documentation to extract functional features and verify system-level coverage.
- Assessment of requirements coverage across five major cybersecurity frameworks.

© Critical Software

CASE STUDY| ENERGY:

BUILDING AN AUDIT-READY CYBERSECURITY BASELINE

The Results

Over 500 system requirements were validated, refined, and linked to stakeholder requirements. Coverage validation across 10 systems and between 1,000 and 1,500 functional features uncovered implementation gaps affecting approximately 50% of assessed features — enabling the customer to identify critical traceability and documentation issues before audit exposure materialized. Northbound traceability gaps were closed; southbound traceability gaps were identified, evaluated, and documented.

A story of success

The intervention transformed a fragmented, high-risk requirements repository into a structured, compliant, and audit-ready cybersecurity baseline — one the customer can defend with confidence.

To find out more about our work
please get in touch: info@criticalsoftware.com

